

TABLE OF CONTENTS

| | |
|---|-------|
| INTRODUCTION | 1-2 |
| SCOPE | 2 |
| PROJECT FINANCING RESPONSE | 2 |
| FOLLOW-UP REVIEW RESULTS | |
| Retention of Tape Logs | 2-3 |
| Local Office Logs | 3-4 |
| Improper Storage of Federal Tax Data | 4-5 |
| Offsite Contractor Access to Records | 5-6 |
| Internal Inspections of Field Offices | 6-7 |
| Staff Knowledge of Confidentiality Requirements | 7-9 |
| Consolidated Print Center Document Destruction | 9 |
| Retention of Destruction Logs at Local Offices | 10 |
| Password Length and Reuse Cycle | 11-12 |
| Audit Trails | 12 |
| Security Testing | 12-13 |
| Trusted Facility Manual | 13 |
| Design Documentation | 14 |
| Encryption Methodology | 14-15 |

INTRODUCTION

The Office of Internal Audit (OIA) performed a follow-up review between the period of October 1, 2004 and April 30, 2005 to determine if the Department of Human Services (DHS) had complied with recommendations pertaining to Central Office IRS Security reported in the IRS' Safeguard Review Report dated January 17, 2002. We followed-up the findings which we determined to be material and still relevant based upon our evaluation of the findings, recommendations, IRS discussion, DHS responses and IRS Comments.

Disclosure of tax return information to Federal, State and Local agencies by the Internal Revenue Service (IRS) and the Social Security Administration (SSA) for use in the Temporary Assistance for Needy Families (TANF), Medicaid, and Food Stamp programs is authorized by Internal Revenue Code (IRC) section 6103(l)(7). The return information is disclosed solely for the purpose of, and to the extent necessary in, determining eligibility for, or the correct amount of benefits under the specified programs. The return information furnished under IRC 6103(l)(7) may not be disclosed to, or exchanged with, or utilized by any other state agency.

The Deficit Reduction Act of 1984 requires states to have an income and eligibility verification system (IEVS) for use in administering the programs. State welfare agencies are required to obtain and utilize Federal tax data from the IRS and the SSA in the verification system. Return information must be independently verified by the client or payer institution before the agency can terminate, deny or reduce any benefits.

As a condition for receiving the return information, recipient agencies are required by IRC 6103(p)(4) to establish and maintain, to the satisfaction of the IRS, certain

safeguards designed to prevent unauthorized uses of the information and to protect the confidentiality of that information.

SCOPE

We interviewed appropriate DHS staff and reviewed pertinent policies, procedures, statutes, a Safeguard Activity Report, and a draft copy of the IRS' Safeguard Review Report for their review performed during the week of July 12, 2004, which we received during the course of our review. We also relied on the results of our own reviews of IRS Security procedures in DHS local and district offices throughout the state, which we performed during the period October 1, 2003 through March 31, 2005.

PROJECT FINANCING RESPONSE

The management of Project Financing has reviewed all findings and recommendations included in this report. They indicated in a memorandum dated June 9, 2005 that they are in general agreement with the report.

FOLLOW-UP REVIEW RESULTS

Retention of Tape Logs

FINDING (Safeguard Review Report Finding # in Parentheses)

1. Magnetic Media that contains Federal tax data is tracked upon receipt and returned to the IRS after processing. (A1, F1)

RECOMMENDATIONS

All logs are to be maintained for five years or the applicable records control schedule, whichever is longer. (A1)

A log needs to be created to document the return/disposal of Federal tax data or several columns can be added to the existing Operations Sheets of the IRS Sheets to capture this information. (F1)

FOLLOW-UP REVIEW CONCLUSION

Project Financing, Program Coordination and Support maintains a tape log to record the dates tapes are received and returned, program number, file and reel number for five years or the applicable records control schedule, whichever is longer. Therefore DHS is in compliance with the recommendations.

Local Office Logs

FINDING

2. Logs are maintained by the local county offices to document any printing of Federal tax data. (A4)

RECOMMENDATION

The guidelines in this section of the PAM 803 should be corrected or clarified. ... The records are to be maintained for five years or the applicable records control schedule, whichever is longer.

FOLLOW-UP REVIEW CONCLUSION

PAM 803, p.5 states that the Designated Staff Person (DSP) must maintain a FIA-4488 (Internal Revenue Service Data Control Sheet) to track notice copies released to specialists. The DSP is to log all notices sent to them on the DHS-4488 and treat them as confidential, shred all notices returned and log the date shredded. PAM 803 further states that the DHS-4488 must be retained for 5 years after the last notice is logged on it and then it may be destroyed by shredding. This complies

with the IRS' recommendation. However, our review of 63 local and district offices revealed that eight of them were not properly completing the DHS-4488 and/or maintaining it for five years.

We have made the appropriate recommendations for retention of the DHS-4488 at the 8 local offices.

Improper Storage of Federal Tax Data

FINDING

3. Paper documents containing Federal tax data are not securely stored in local offices, and Federal Tax Data is commingled with case files in the local offices, therefore not properly identified. (B2, C3, C5)

RECOMMENDATIONS

Documents containing Federal tax data are considered to be items that require a high level of security. Federal tax data must be stored according to the protection standards as outlined in Pub. 1075 (Tax Information Security Guidelines for Federal, State, and Local Agencies). ... As an alternative to locking up the entire case file, the agency should: ... Remove all confidential Federal tax data from case files and lock up in a secure centralized container with access restrictions until it is legally permissible to shred it. (B2)

Federal tax data needs to be identified and removed from case files. (C3)

Until all Federal tax data is removed from opened/closed case files, it must be identified and properly labeled. ... (C5)

FOLLOW-UP REVIEW CONCLUSION

PAM 803, p.4, and Program Policy Bulletin 2002-004, p.7 state that the Unearned Income Notices are not to be filed in the case record but must be returned to the DSP. Also a memo dated June 7, 2002 was sent to all DSP's stating that 2 reports were enclosed (one for open cases and one for closed cases) listing customers who have received IRS notices sometime since November 1999. The memo explained that all the notices must be removed from the case records and forwarded to the DSP to be logged on the DHS-4488 and then shredded. PPB 2002-004, p.8 states that these notices, plus all other IRS data notices located in the case record, must be removed and forwarded to the DSP for logging and destruction.

This complies with the IRS's recommendations. However in 28 of 63 local and district offices we reviewed we found Unearned Income Notices in the case records or caseworkers who indicated they would put the Unearned Income Notices in the case files.

We have made appropriate recommendations for retention and destruction of Unearned Income Notices to all 28 local offices.

Offsite Contractor Access to Records

FINDING

4. Case files retired to an offsite contractor for storage can be retrieved by individual case file when requested. (C4)

RECOMMENDATION

Offsite storage contractors should not have access to Federal tax data. When a case file is to be retrieved from storage, the entire sealed box must be returned. ...

FOLLOW-UP REVIEW CONCLUSION

The memo sent to all DSP's on June 7, 2002 required them to remove all IRS notices received since November of 1999 from all open and closed the case files. The notices were to be removed and forwarded to the DSP for logging and destruction. Therefore, cases retired to an offsite storage facility subsequent to June 7, 2002 should not contain any IRS notices. However, we were informed that there has been no specific action taken regarding case files retired to an offsite contractor that contain IRS notices issued prior to November 1999.

WE RECOMMEND that DHS ensure that offsite storage contractors do not have access to Federal tax information.

Internal Inspections of Field Offices

FINDING

5. Internal Inspections are being conducted by DHS for field offices. (D1)

RECOMMENDATION

We need additional information, such as copies of the internal inspection questionnaire and work file before further commenting on this issue. ...

Also, the IRS commented that the key areas that should be addressed include: record keeping, secure storage, limited access, disposal, and computer security.

FOLLOW-UP REVIEW CONCLUSION

Our current audit guidelines assess whether the local office is in compliance with IRS security guidelines for confidentiality in storing and releasing confidential material on clients' unearned income, and address record keeping, secure storage,

limited access, disposal, and computer security. Therefore DHS is in compliance with the recommendation.

Staff Knowledge of Confidentiality Requirements

FINDING

6. Department employees in the field offices were unfamiliar with confidentiality requirements and sanctions for unauthorized disclosure of Federal tax data; related initial certification and annual recertification are not documented; and employees were unaware of the Taxpayer Browsing Protection Act. (D2, 3, 4)

RECOMMENDATIONS

A greater awareness of what constitutes FTI (Federal Tax Information) needs to be implemented throughout the department – advising employees of the civil and criminal sanctions imposed for unauthorized disclosure of Federal tax data. It is recommended that security and safeguarding requirements be periodically discussed at group meetings or in memos to the appropriate personnel. Also, the IRS Publication 1075 provides additional suggestions for use by your department. (D2)

We ask that the department develop and implement a document for initial certification and annual recertification. The initial certification and recertification should be documented and placed in the department's files for review. (D3)

As part of the certification and at least annually afterwards, employees should be advised of the provisions of the IRC 7213(a), 7213A, and 7431. (D4)

FOLLOW-UP REVIEW CONCLUSION

DHS has taken steps to make appropriate personnel aware of confidentiality requirements and the sanctions imposed for unauthorized disclosure of Federal tax data. L-letter L-04-044, dated April 7, 2004 from the DHS Deputy Director of Field Services Administration was addressed to the County Directors and District Office Managers throughout the State. This memo:

- Informs the County Directors and District Office Managers that the IRS requires safeguard measures to ensure the confidentiality of the Federal Tax Information (FTI).
- States that certifying that each employee understands DHS's procedures for safeguarding FTI should precede granting employees access to FTI and they should be required to maintain their authorization to access FTI through annual recertification. It also states that the initial certification and recertification should be documented and placed in the agency's files for review.
- States that the local offices should make employees aware that disclosure restrictions and the penalties apply even after employment with the agency has ended.
- Listed a variety of methods that security information and requirements can be expressed to appropriate personnel.

The memo also referred to PAM 803 regarding DHS policy for Safeguarding IRS information. PAM 803, p.1 refers to criminal and civil penalties for unauthorized disclosure of tax return information per Sections 7213(a) and 7431 of the Internal Revenue Code. These Sections are included in PAM 803 as well as Section 7213A, which discusses the unauthorized inspection of FTI referred to in the Taxpayer Browsing Protection Act. The memo also refers to Publication 1075 (Tax Information Security Guidelines for Federal, State, and Local Agencies), which

contains safeguards for protecting Federal tax returns and return information. This memo addresses findings D2, 3, 4 of the report. Therefore DHS is in compliance with the recommendations.

Consolidated Print Center Document Destruction

FINDING

7. Paper documents in the Consolidated Print Center (CPC) containing Federal tax data are not being disposed of according to the requirements in Publication 1075. (F3)

RECOMMENDATION

Federal tax data must never be disclosed to contractors during disposal unless authorized by the IRC (Internal Revenue Code). If a contractor is going to be used to dispose of these documents, then a department employee should witness destruction.

FOLLOW-UP REVIEW CONCLUSION

We were informed that in the CPC bad/ruined prints containing FTI are placed in general shred containers and a contractor is used for destruction. There is no monitoring of the destruction process by department employees. We concluded that DHS has not complied with this recommendation.

WE RECOMMEND that DHS maintain a separate secured shred container for bad/ruined prints containing FTI, and that a DHS employee witness document destruction.

Retention of Destruction Logs at Local Offices

FINDING

8. Destruction logs are not being used to record the disposition of paper documents containing Federal tax data. (F5)

RECOMMENDATION

We ask that the department establish logs to record the destruction of Federal tax data. The information in these logs should be adequate to identify the material destroyed and the date and manner of destruction.

FOLLOW-UP REVIEW CONCLUSION

PAM 803, p.3 states that if the unearned income notice (notice) is not returned to the customer it must be sent to the Designated Staff Person (DSP) for logging and destruction. Also on page 5 it states that the DSP is to log all notices received on the DHS-4488 (Internal Revenue Service Data Control Sheet) and shred all notices received and log the date shredded. Further, the Program Policy Bulletin 2002-004, p.7-8; the PAM 803 Desk Aids, “Specialist Processing of IRS Matches” and “DSP Duties”; and the “Internal Control Criteria for Local Office Operations” all state that the notices must be returned to the DSP for logging and destruction. Therefore Central Office has taken action to ensure that logs to record the destruction of FTI are established. However, our review of 63 local and district offices revealed that eight of them were not properly completing the FIA-4488 and/or maintaining it for five years.

We have made the appropriate recommendations to the 8 local offices that were out of compliance.

Password Length and Reuse Cycle

FINDING

9. The minimum password length is set at four characters and the password reuse cycle is set at two. (H5)

RECOMMENDATION

Weak passwords are easy for an intruder or other unauthorized individual to guess and we are concerned about the system setting of four characters as the minimum acceptable password length. The minimum password length should not be less than six characters. In order to prevent users from reusing a password within a six-month period, we also recommend that the history cycle be increased to a number that would deter the user from trying to reuse the same password.

FOLLOW-UP REVIEW CONCLUSION

DHS has not complied with this recommendation. In its draft report, IRS states: “FIA and DIT (Department of Information Technology) should adopt and enforce the password policies that are prescribed by the security policy. The policies should cover the following (if applicable):

- Minimum password length of eight characters
- Minimum of two numbers, mixed case letters and special characters
- Maximum password age of 180 days
- Minimum password age of 5 days
- Minimum password history of 5
- Prohibit the use of usernames within a password
- Prohibit the use of dictionary words or common passwords
- Prohibit the use of words from a customized dictionary.

- Users are forced to change their initial passwords during first login.”

DHS will be required to submit a corrective action plan to the IRS for this finding.

Audit Trails

FINDING

10. Audit trails may require revision. (H6)

RECOMMENDATION

Both DIT and DHS should ensure that audit trails contain security-relevant events for the mainframe and LAN. Logon attempts, both successful and unsuccessful, and password changes should be recorded in an audit record. Audit records relating to security events should be reviewed periodically (at least weekly is preferred) for anomalies. Audit records relating to specific accesses to FTI should also be maintained for 5 years.

FOLLOW-UP REVIEW CONCLUSION

We were informed by the IRS that the auditing controls now appear to be functioning with sufficient operating effectiveness. Therefore DHS is in compliance with the recommendation.

Security Testing

FINDING

11. Security testing is conducted, however, documentation was not available during the review. (H7)

RECOMMENDATION

Security features on systems that process or transmit FTI should be tested periodically. Testing units within DIT and DHS should coordinate their efforts to ensure that the appropriate security features on the systems within their area of responsibility are tested. Testing should also be documented.

FOLLOW-UP REVIEW CONCLUSION

We were informed by the IRS that the department now meets the security testing requirements.

Trusted Facility Manual

FINDING

12. A trusted facility manual is in place, however, certain documentation may require refinement. (H8)

RECOMMENDATION

Auditing features on both the mainframe and LAN need to be enhanced to meet the security class C2 requirements, therefore, the Trusted Facility Manual (TFM) should be revised to include a section describing the audit mechanisms and procedures. DIT and DHS should coordinate their efforts to ensure that the TFM contains the procedures for examining and maintaining audit files as well as the detailed audit record structure for each type of audit event. ...

FOLLOW-UP REVIEW CONCLUSION

We were informed by the IRS that the department now meets the TFM requirements.

Design Documentation

FINDING

13. Design documentation was not available. (H10)

RECOMMENDATION

Since this issue was identified in the last review, we request that a copy of the above documentation be sent to this office within 30 days of the date on the letter that accompanied this report. ...

FOLLOW-UP CONCLUSION

The department stated in its response to the finding that diagrams were provided to the IRS auditor. The IRS' follow-up comment stated that the department's response was acceptable. Also, we were informed by the IRS during the course of our follow-up review that the department now meets the design documentation requirement.

Encryption Methodology

FINDING

14. An encryption methodology is not in place for transmitting FTI. (H11)

RECOMMENDATION

Access to the mainframe and LAN password files should be monitored more closely. All accesses to the file should be monitored by an administrator that does not have access rights to this file. If the capability exists, the audit reduction tool, Audit Reporting Utility (ARU), should be configured to identify all accesses and ensure that they go to the proper reviewing official.

The department should continue to explore encryption technology. The product line should provide Level 2, FIPS Pub 140-2 cryptographic protection in its implementation of 3DES (FIPS PUB 46-3). ...

FOLLOW-UP REVIEW CONCLUSION

We were informed by the IRS that FTI transmissions over telecommunication circuits between state offices and the DIT data center appear to comply with Treasury-Approved guided media techniques and Treasury-Approved Protected Network Services.

Publication 1075, p.22 states that the two acceptable methods of transmitting FTI over telecommunication devices are the use of encryption or the use of guided media. Therefore the department has an acceptable method in place for transmitting FTI.